privatim
Konferenz der schweizerischen Datenschutzbeauftragten
Conférence des préposé(e)s suisses à la protection des données
Conferenza degli incaricati svizzeri per la protezione dei dati

Transfert de données personnelles à des organisations aux États-Unis sur la base du Swiss-U.S. Data Privacy Framework

1 Résumé

Les organisations privées, qui sont certifiées conformément au Data Privacy Framework en vigueur entre la Suisse et les États-Unis (Swiss-U.S. DPF)[1], offrent un niveau de protection des données adéquat.

Dans le contexte de l'externalisation des données à des organisations certifiées, privatim émet les trois recommandations suivantes à l'attention des organes publics cantonaux et communaux :

1. **Vérification** : il convient de vérifier la situation juridique en lien avec le Swiss-U.S. DPF (https://www.dataprivacyframework.gov/list) au moment d'un transfert planifié de données personnelles à une organisation privée aux États-Unis ;
2. **Validité du certificat** : Vérification périodique de la validité du certificat, la révocation ou le non-renouvellement du certificat par le destinataire des données étant possible en tout temps ;
3. **Scénario de sortie** : prévoir un scénario de sortie lors de l'externalisation du traitement des données personnelles à une organisation certifiée selon le Swiss-U.S. DPF.

2 Contexte

Le Conseil fédéral, dans son ordonnance du 14 août 2024, a admis, sous réserve, les États-Unis sur la liste figurant dans l'annexe 1 de l'Ordonnance sur la protection des données (OPDo ; RS 235.11) où sont répertoriés les États, les territoires, les secteurs déterminés dans un Etat et les organismes internationaux dans lesquels un niveau de protection des données adéquat est garanti.[2] La réserve indique toutefois qu'un niveau de protection adéquat dans le domaine de la protection des données selon l'art. 16 al. 1 LPD (RS 235.1) ne peut être attesté qu'aux organisations privées certifiées, conformément au Data Privacy Framework (Swiss-U.S. DPF)[3] en vigueur à ce moment-là entre la Suisse et les États-Unis. La certification relevant du Swiss-U.S. DPF consiste en une auto-certification de

[1] Disponible à l'adresse suivante : https://www.dataprivacyframework.gov/EU-US-Framework => Suisse (état : 3 mars 2025).

[2] Ordonnance sur la protection des données (OPDo), modification du 14 août 2024, RO 2024 435.

[3] Disponible à l'adresse suivante : https://www.dataprivacyframework.gov/EU-US-Framework => Suisse (état : 3 mars 2025).

privatim
c/o Préposé à la protection des données du canton de Berne
Poststrasse 25, 3072 Ostermundigen
Tél. +41 (31) 633 74 10
praesident@privatim.ch, www.privatim.ch

l'organisation privée concernée à renouveler chaque année en vertu du chapitre 3, chiffre 6 Swiss-U.S. DPF. Une liste des organisations certifiées peut être consultée en ligne.[4]

Le décret exécutif 14086 (Executive Order ; EO) du 7 octobre 2022 constitue une autre base de l'attestation d'adéquation. Il s'agit d'une directive contraignante du président, qui règle l'exécution des tâches par l'exécutif. Concrètement, l'EO 14086 introduit certaines mesures visant à améliorer la protection du droit face aux services de renseignements. Il prévoit notamment une procédure de recours à deux niveaux pour les personnes issues d'États qualifiés.[5] Cette procédure permet de contrôler la collecte des données personnelles par les services de renseignements par le biais du Civil Liberties Privacy Officer et de la Data Protection Review Court en respectant la législation américaine. L'EO 14086 garantit une certaine indépendance personnelle et matérielle à ces deux instances.[6]

L'attestation portant sur la protection adéquate des données pour les entreprises certifiées en vertu du Swiss-U.S. DPF sert de base à la communication des données vers l'étranger selon l'art. 16 LPD et est contraignante pour les organismes fédéraux et les privés. D'un point de vue juridique et matériel, elle représente une évaluation généralisée des risques par le Conseil fédéral, sur la base de laquelle le transfert de données personnelles entre la Suisse et les États-Unis peut avoir lieu sans autres garanties de la part du destinataire au sens de la protection des données.

Pour les organismes publics des cantons et des communes, l'attestation n'a pas toujours une portée directe juridiquement obligatoire, mais elle constitue, de manière générale, une base suffisante pour la reconnaissance d'un niveau de protection des données adéquat pour les communications, de même qu'un critère possible pour l'analyse d'impact de la protection des données dans le cas d'externalisation transfrontière de traitements de données. Toutefois, les organismes publics des cantons et des communes restent juridiquement responsables de l'évaluation des risques dans chaque cas concret.

3 Effets juridiques de la certification

3.1 Communication facilitée des données personnelles aux entreprises certifiées

Toute organisation privée s'engage, par la certification, à respecter les principes du Swiss-U.S. DPF lors du traitement des données personnelles qui lui sont communiquées depuis la Suisse. Il s'agit des principes primaires mentionnés ci-dessous dans la partie II du Swiss-U.S. DPF, qui, pour leur part, sont complétés par d'autres principes dans la partie III.

- *Notice*. Un devoir d'informer exhaustif qui comprend, notamment, la certification de l'organisation et d'autres sous-organisations, l'obligation de respecter les principes

---

4 Disponible à l'adresse suivante : https://www.dataprivacyframework.gov/list (état : 3 mars 2025).

5 Par le courrier du procureur général des États-Unis du 7 juin 2024 et en se fondant sur la reconnaissance d'un niveau de protection des données adéquat par le Conseil fédéral, la Suisse a été reconnue comme étant un Etat qualifié, disponible en ligne à l'adresse suivante : https://www.justice.gov/opcl/media/1355326/dl?inline (état : 4 mars 2025).

6 Voir le rapport explicatif de l'OFFICE FÉDÉRAL DE LA JUSTICE, Evaluation de l'adéquation – États-Unis – Établissement d'un cadre pour le transfert de données personnelles depuis la Suisse vers les organisations certifiées aux États-Unis (Swiss-U.S. Data Privacy Framework) – Évaluation de l'adéquation du niveau de protection des données personnelles, voir 25 et ss., disponible à l'adresse suivante : https://www.newsd.admin.ch/newsd/message/attachments/89020.pdf (état : 4 mars 2025).

de la protection des données, l'objectif de la collecte des données personnelles, les droits des personnes concernées, les personnes de contact pour défendre ces droits, l'instance de règlement des litiges désignée, gratuite et indépendante, la possibilité d'un arbitrage contraignant et la responsabilité en matière de communication abusive à des tiers.

- *Choice*. Concerne la nécessité du consentement et les exigences légales pour le transfert des données à des tiers ou pour des modifications de finalité.
- *Accountability for Onward Transfer*. Règle les conditions de la communication à des tiers sous mention des deux premiers principes et du respect de la finalité et de la garantie d'un niveau équivalent de protection des données par les tiers.
- *Security*. Concerne le principe de la sécurité des données et de l'évaluation sur la base des risques, qui découlent de la nature du traitement et des données personnelles.
- *Data Integrity and Purpose Limitation*. Définit les principes de la minimisation des données et des aspects de l'exactitude des données pour ce qui est de la finalité du traitement. En particulier, le principe comprend aussi une composante temporelle selon laquelle le caractère personnel des données qui ne sont plus requises doit être supprimé. Le principe est soumis, notamment, à la réserve découlant d'intérêts contraires tels que le traitement en vertu d'un intérêt public ou dans le cadre du journalisme ou de l'art.
- *Access*. Le droit en matière de protection des données de demander des renseignements sur ses propres données personnelles disponibles et, le cas échéant, leur modification ou leur effacement.
- *Recourse, Enforcement and Liability*. Obligation de mettre en place des mécanismes efficaces pour garantir le respect de ces principes.

En interaction avec l'environnement réglementaire créé par les bases légales mentionnées dans la décision d'adéquation du Conseil fédéral, la certification a pour conséquence que l'on atteste à l'organisation concernée un niveau de protection des données adéquat pour la communication transfrontière des données personnelles. Cela permet une communication des données à cette organisation aux États-Unis en vertu de l'art. 16, al. 1, LPD.

3.2 Externalisation des traitements des données à des entreprises certifiées

La décision d'adéquation du Conseil fédéral n'a pas la même valeur juridique pour l'externalisation de traitements des données – qu'elle soit classique ou dans le cloud – que lors de communications de données à l'étranger. Cela s'explique par le fait que l'organisme public qui effectue l'externalisation reste toujours responsable en vertu de la législation sur la protection des données. Par conséquent, le transfert des données, qui doit nécessairement avoir lieu dans le cas d'une externalisation, est en principe, possible, tandis qu'un traitement des données par le destinataire aux fins de l'exécution des tâches de l'organisme public qui effectue le transfert doit être réglé en même temps par contrat.

Les dispositions usuelles en matière de législation sur la protection des données s'appliquent à cette règlementation contractuelle, tout comme à l'externalisation sur le territoire suisse, en particulier la protection contractuelle des droits des personnes concernées en matière de protection des données, le droit de l'organisme public de donner

des instructions, l'adoption d'obligations applicables en droit suisse de la protection des données par le destinataire et la prise en charge de la surveillance par l'autorité compétente chargée de la protection des données. L'aide-mémoire Risque et mesures spécifiques au Cloud[7] contient d'autres informations sur les conditions-cadres, indépendantes de la décision d'adéquation, en vigueur lors de l'externalisation qui a recours à une solution Cloud.

En ce qui concerne la protection contractuelle des droits des personnes concernées, il faut veiller à ce que les efforts pour faire valoir ces droits correspondent à peu près à ceux consentis pour l'exercice de ces droits sur le territoire suisse. Il en va de même lorsqu'il s'agit de se prévaloir des droits contractuels de l'organe public qui sont nécessaires à la défense des droits des personnes concernées. C'est la raison pour laquelle l'externalisation transfrontière du traitement des données personnelles par des organismes publics nécessite, en règle générale, de choisir la législation suisse et un for en Suisse afin de répondre aux exigences de la proportionnalité du traitement des données.

L'environnement institutionnel qui permet son application est déterminant pour l'efficacité du Swiss-U.S. DPF. Sans mécanismes d'application efficaces, le DPF n'est pas en mesure d'offrir la réduction des risques espérée pour l'externalisation aux États-Unis. A cet effet, il faut veiller à ce que les conditions de l'externalisation restent stables pendant toute la durée prévue de celle-ci. Ce qui signifie que la certification du mandataire, les conventions en matière de droit de la protection des données et l'efficacité de l'environnement institutionnel nécessaire à son application doivent être assurés pendant la durée de l'externalisation. Pour ces raisons il convient d'élaborer un scénario de sortie qui permette, le cas échéant, la poursuite du traitement des données conformément à la protection des données.

Dans cet ordre d'idées, le communiqué de presse du 27 janvier 2025 du Privacy and Civil Liberties Oversight Board est important vu que le président a licencié trois des quatre membres du Privacy and Civil Liberties Oversight Board (PCLOB), dont le Chair.[8] De ce fait, le Board ne peut pas atteindre le quorum de trois membres pour certaines décisions. Dans le cadre du DPF, le PCLOB possède un droit de consultation lors de la sélection des juges de la Data Protection Review Court, ainsi que la surveillance du respect de l'EO 14086 par les services secrets. Un premier rapport est prévu en 2025.[9]

4 Conclusion

Au vu de la volatilité de l'environnement institutionnel du DPF et des mesures d'économie du gouvernement américain en vigueur actuellement, on ne sait pas combien de temps les bases de la décision d'adéquation du Conseil fédéral conserveront leur validité.[10] Par

---

7 Disponible à l'adresse suivante : https://www.privatim.ch/fr/nouvelle-version-revisee-de-laide-memoire-risques-et-mesures-specifiques-au-cloud-de-privatim/ (état : 16 avril 2025).

8 https://documents.pclob.gov/prod/Documents/EventsAndPress/994df0d6-6bae-4284-a95f-3f3699e0a0f0/PCLOB%20press%20release%20(1-27-25)%20-%20508%20Complete.pdf

9 https://documents.pclob.gov/prod/Documents/EventsAndPress/6e6c7a7b-6036-4d6d-b635-ffb53f68e4f4/Statement%20on%20PCLOB%20Review%20Under%20Section%203%20of%20EO%14086,%20Completed%20508,%20Nov%207%202024.pdf

10 Dans un entretien datant du 13 mars 2025, Michael McGrath, Commissaire européen compétent en la matière, a souligné le fait que l'UE s'en tenait au DPF, mais que la Commission observait de près l'évolution des mécanismes d'application aux États-Unis ; voir : https://www.csis.org/analysis/future-transatlantic-digital-collaboration-eu-commissioner-michael-mcgrath (état : 24 avril 2025).

conséquent, au moment d'un transfert prévu de données personnelles à une organisation privée aux Etats-Unis, il convient de vérifier la situation juridique dans le domaine du Swiss-U.S. DPF.

Pour pouvoir réagir à de futurs changements, les processus, qui prévoient une externalisation du traitement des données personnelles à une organisation certifiée selon le Swiss-U.S. DPF, devraient être aménagés d'une manière qui permette de prendre des mesures efficaces pour protéger les personnes concernées dans le cas d'une réduction importante du niveau de protection selon la législation sur la protection des données et/ou de déplacer les traitements de données en question vers un pays qui dispose d'un niveau de protection des données adéquat. Un scénario de sortie réaliste pouvant être mis en place si besoin est indispensable. Il faut tenir compte, en particulier, des changements survenant dans les domaines suivants :

- la révocation ou le non-renouvellement du certificat par le destinataire ;
- la modification ou l'abrogation des bases légales y relatives dans la législation américaine ;
- l'efficacité de la procédure de recours à deux niveaux ;
- la capacité d'agir des autorités de surveillance.

A cet égard, il convient de noter que le Conseil fédéral, dans le cadre de la vérification continue des conditions selon l'art. 16, al. 1, LPD, en lien avec l'art. 8 OPDo, est habilité à révoquer, le cas échéant, la décision d'adéquation.

Il en découle la nécessité de vérifier régulièrement les analyses d'impact de la protection des données dans le cadre d'externalisation de traitements des données vers les Etats-Unis. Dans ce cadre, il y a lieu de considérer les modifications dans les bases matérielles et institutionnelles sur lesquelles s'appuie la décision d'adéquation du Conseil fédéral, les modifications de leur application par les autorités américaines et/ou dans la jurisprudence concernée et les mesures du gouvernement américain, qui portent atteinte au financement ou à l'efficacité des instances de recours et/ou de surveillance. En conséquence, il faut réévaluer les bases légales suivantes mentionnées dans la décision de modification du Conseil fédéral du 14 août 2024, ainsi que les institutions établies par elles lorsque les circonstances l'exigent :

- Swiss-U.S. Data Privacy Framework Principles Issued by the U.S. Department of Commerce[11] ;
- décret exécutif 14086 (Executive Order du président des Etats-Unis ; EO) du 7 octobre 2022[12] ;
- règlement de la cour en matière d'examen de la protection des données du procureur général des États-Unis du 7 octobre 2022[13] ;

[11] Disponible à l'adresse suivante : https://www.dataprivacyframework.gov/EU-US-Framework => Suisse (état : 3 mars 2025).

[12] Disponible à l'adresse suivante : https://www.federalregister.gov/documents/2022/10/14/2022-22531/enhancing-safeguards-for-united-states-signals-intelli-gence-activities (état : 3 mars 2025).

[13] Disponible à l'adresse suivante : https://www.federalregister.gov/documents/2022/10/14/2022-22234/data-protection-review-court (état : 3 mars 2025).

- directive 126 de la communauté de renseignement portant sur l'EO 14086[14] ;
- reconnaissance de la Suisse comme étant un Etat qualifié eu égard à la légitimation du mécanisme de recours selon le paragraphe 3 de l'Executive Order 14086 par le procureur général américain du 7 juin 2024[15].

[14] Disponible à l'adresse suivante : https://www.dni.gov/files/documents/ICD/ICD_126-Implementation-Procedures-for-SIGINT-Redress-Mechanism.pdf (état : 3 mars 2025).

[15] Disponible à l'adresse suivante : https://www.justice.gov/opcl/media/1355326/dl?inline (état : 3 mars 2025).